

CLIPPEDIMAGE= JP02000181871A

PAT-NO: JP02000181871A

DOCUMENT-IDENTIFIER: JP 2000181871 A

TITLE: DEVICE AND METHOD FOR AUTHENTICATION

PUBN-DATE: June 30, 2000

INVENTOR-INFORMATION:

NAME COUNTRY

TIMOTHY, ALAN DIETZ N/A

ASSIGNEE-INFORMATION:

NAME COUNTRY

INTERNATL BUSINESS MACH CORP <IBM> N/A

APPL-NO: JP11349691

APPL-DATE: December 9, 1999

INT-CL_(IPC): G06F015/00; G06F019/00 ; G06F017/30 ; H04L009/32

ABSTRACT:

PROBLEM TO BE SOLVED: To enable a safe transaction by decoding a user request into living body measurement data at a remote place by using an open key and confirming biological measurement data in order to authenticate a user request.

SOLUTION: The user inputs living body measurement data (fingerprint, etc.), through a biometric input sensor 62. An encryption processor assembly(EPA) 58 enciphers a combination of biometric data and transaction data by using a key K1 and adds the ID of the EPA 58 to a request message. The message is sent to a credit server 70. The server 70 uses EPAID to retrieve the key K2 of the user associated with a data base 72 and deciphers the message with the key K2. A confirming function 80 retrieves user data from a biometric data base 74 by using the biometric part of the message, makes an authentication decision, and enciphers the replay with the key K2. The server 70 sends the reply to the user.

COPYRIGHT: (C)2000,JPO

(11)特許出願公開番号

特開2000-181871

(P2000-181871A)

(43)公開日 平成12年6月30日(2000.6.30)

(51) Int.Cl.?

識別記号

FI

テーマコード・(参考)

G O 6 F 15/00

3 3 0

G O 6 F 15/00

330 F

19/00

15/30

3 3 0 E

17/30

15/40

330

H04L 9/32

H 0 4 L 9/00

6 7 3 D

審査請求 有 請求項の数20 OL (全 14 頁) 最終頁に続く

(21)出願番号

特願平11-349691

(22) 出願日

平成11年12月9日(1999.12.9)

(31)優先權主張番号 09/213324

(32)優先日 平成10年12月16日(1998.12.16)

(33)優先權主張国 米国 (US)

(71)出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション

INTERNATIONAL BUSINESS
MACHINES CORPORATION

アメリカ合衆国10504、ニューヨーク州
アーモンク (番地なし)

(72)発明者 ティモシー・アラン・ディエツ

アメリカ合衆国78717 テキサス州、オースティン、ヴァロナ・ドライブ
10004

(74) 代理人 100086243

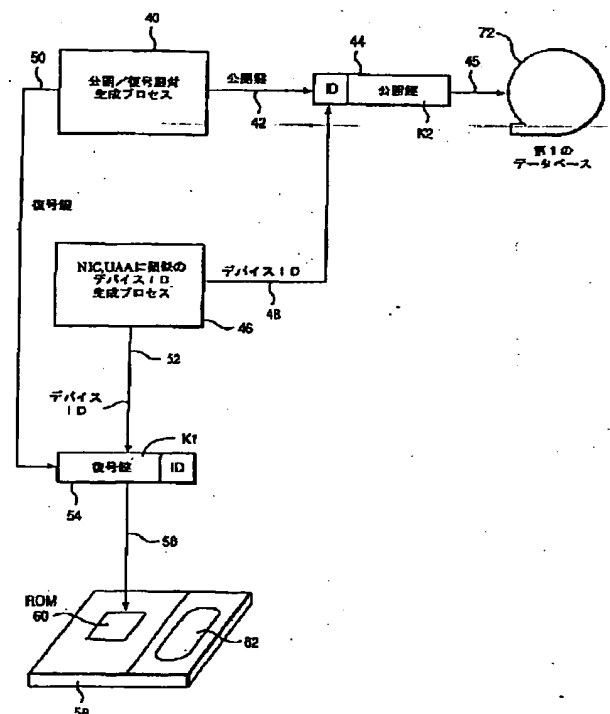
弁理士 坂口 博 (外1名)

(54) 【発明の名称】 認証方法及び装置

(57) 【要約】

【課題】 コンピュータ・システムのセキュリティ技術、特に遠隔地からの要求およびメッセージを認証するための方法、装置、およびコンピュータ・プログラム・プロダクトを提供。

【解決手段】方法、装置、およびコンピュータ・プログラム。プロダクトは、復号鍵および公開鍵を生成し、ユーザに対応する生物測定的データを生成し、遠隔地で生物測定的データと公開鍵とを記憶し、復号鍵によって暗号化された生物測定的データを含むユーザ要求を局所で生成し、遠隔地にユーザ要求を伝送し、遠隔地で公開鍵を用いてユーザ要求を生物測定的データに解釈し、記憶された生物測定的データを検索し、さらにユーザ要求を認証するために生物学的測定データを確認する。



【特許請求の範囲】

【請求項1】コンピュータ・システム・ネットワークでユーザの要求を認証するための方法であって、
復号鍵および公開鍵を生成するステップと、
前記ユーザに対応する生物測定データを生成するステップと、
遠隔地で前記生物測定データと前記公開鍵とを記憶するステップと、
前記復号鍵によって暗号化された前記生物測定データを含む前記ユーザ要求を局所で生成するステップと、
前記遠隔地に前記ユーザ要求を伝送するステップと、
前記遠隔地で前記公開鍵を用いて前記ユーザ要求を前記生物測定データに解読するステップと、
前記記憶された生物測定データを検索するステップと、
前記ユーザ要求を認証するために前記生物学的測定データを確認するステップと、
を有することを特徴とする方法。

【請求項2】前記生物学的測定データを確認するステップは、前記解読されたユーザ要求に送られた前記生物測定データと前記記憶された生物測定データとを比較することを、含むことを特徴とする請求項1に記載の方法。

【請求項3】前記ユーザ要求の伝送は、前記局所と前記遠隔地とを相互接続するネットワーク上であることを特徴とする請求項2に記載の方法。

【請求項4】前記復号鍵に対応付けられたID番号を持つ前記遠隔地の前記復号鍵を記憶するステップを、さらに有することを特徴とする請求項3に記載の方法。

【請求項5】前記ID番号は前記公開鍵に対して一意に対応付けされており、前記方法はさらに、
前記ID番号および前記公開鍵を前記遠隔地の第1のデータベースに組として記憶するステップを有することを特徴とする請求項4に記載の方法。

【請求項6】前記生物測定データは第2のデータベースに記憶されていることを特徴とする請求項5に記載の方法。

【請求項7】前記ユーザおよび前記生物測定データに対応付けられたデータ・フィールドを生成するステップと、
前記生物測定データと前記データ・フィールドとを組として前記第2のデータベースに記憶するステップと、
をさらに有することを特徴とする請求項6に記載の方法。

【請求項8】前記復号鍵を記憶するステップは、前記局所で行われることを特徴とする請求項7に記載の方法。

【請求項9】前記生物測定データを生成するステップは、前記局所で行われることを特徴とする請求項8に記載の方法。

【請求項10】前記確認に応じて前記要求を処理するステップをさらに有することを特徴とする請求項9に記載の方法。

【請求項11】コンピュータ・システム・ネットワークでユーザの要求を認証する装置であって、
復号鍵および公開鍵を生成する手段と、
前記ユーザに対応する生物測定データを生成する手段と、
遠隔地で前記生物測定データと前記公開鍵とを記憶する手段と、
前記復号鍵によって暗号化された前記生物測定データを含む前記ユーザ要求を局所で生成する手段と、
前記遠隔地に前記ユーザ要求を伝送する手段と、
前記遠隔地で前記公開鍵を用いて前記ユーザ要求を前記生物測定データに解読する手段と、
前記記憶された生物測定データを検索する手段と、
前記ユーザ要求を認証するために前記生物学的測定データを確認する手段と、
を有することを特徴とする装置。

【請求項12】前記生物学的測定データを確認する手段は、前記解読されたユーザ要求に送られた前記生物測定データと前記記憶された生物測定データとを比較する手段を含むことを特徴とする請求項11に記載の装置。

【請求項13】前記ユーザ要求を伝送する手段は、前記局所と前記遠隔地とを相互接続するネットワーク上であることを特徴とする請求項12に記載の装置。

【請求項14】前記復号鍵に対応付けられたID番号を持つ前記遠隔地の前記復号鍵を記憶する手段を、さらに有することを特徴とする請求項13に記載の装置。

【請求項15】前記ID番号は前記公開鍵に対して一意に対応付けされており、前記装置はさらに、
前記ID番号および前記公開鍵を前記遠隔地の第1のデータベースに組として記憶する手段を有することを特徴とする請求項14に記載の装置。

【請求項16】前記生物測定データを前記遠隔地で第2のデータベースに記憶する手段をさらに有することを特徴とする請求項15に記載の装置。

【請求項17】前記ユーザおよび前記生物測定データに対応付けられたデータ・フィールドを生成する手段と、
前記生物測定データと前記データ・フィールドとを組として前記第2のデータベースに記憶する手段と、
をさらに有することを特徴とする請求項16に記載の装置。

【請求項18】前記復号鍵の記憶は、前記局所で行われることを特徴とする請求項17に記載の装置。

【請求項19】前記生物測定データの生成は、前記局所で行われることを特徴とする請求項18に記載の装置。

【請求項20】前記確認に応じて前記要求を処理する手段をさらに有することを特徴とする請求項19に記載の装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータ・システムのセキュリティ技術、特に遠隔地からの要求およ

びメッセージを認証するための認証機構に関し、特に認証を行うための方法、装置、およびコンピュータ・プログラム・プロダクトに関する。

【0002】

【従来の技術】公開／復号鍵対およびユーザID／パスワードはコンピュータ・システムの認証スキームで現在用いられている現代認証機構の基本的側面である。これらの基本的側面は、特定の一本のソフトウェア、例えばよく知られているLotus Notes (IBM Corporationの登録商標) アプリケーションまたは安定したウェブ・ブラウザによって使用されるハードウェアに存在しているデジタル証明書を介して元来特定のデバイスに結びつけられている。ハードウェア・セキュリティに穴がかけられないようにセキュリティの層を追加するために、しばしばユーザIDおよびパスワードが使用される。特定のデバイスの物理的使用とユーザIDおよびパスワードについての認識との組み合わせは、過去においてユーザの認証を保証するのに十分なものと見なされていた。

【0003】しかし、セキュリティに穴を開けるためのますます高度化する技術および情報に耐えようとする現代のセキュリティ・システムに対する絶え間ない攻撃によって、今ではそのようなシステムの機能が十分満足できるものではないことが嘆かわしいほどに明らかになった。例えば、万一ユーザIDおよびパスワード・データの信用が損なわれはじめ、またデバイスが公然とアクセス可能あるいは容易に紛失または盗難されやすくなると、例えばパーソナル・コンピュータまたはパーソナル・デジタル・アシスタント (PDA) の場合、不正な使用によってユーザの権利が悲惨な結果となる。

【0004】

【発明が解決しようとする課題】したがって、公用設定で実施される安全なトランザクションを可能とするために、特に普及しているデバイス、例えば前述のPDA、自動窓口機 (ATM)、キオスク等の様々な専用ネットワークあるいは公用ネットワーク、企業や他の事業実体のあいだで好評を博して展開されているイントラネットまたはインターネットそれ自体等を介して、そのような驚異を防ぐことができる技術の適用が緊急に求められている。

【0005】

【課題を解決するための手段】適当なデバイスには、公開／復号鍵対が割り当てられ、また製造業者における指紋スキャニング・パッド等の生物測定データ入力デバイスが備え付けられている。指紋や網膜などの生物測定データは、ユーザの身元を確認するために、ネットワーク・コンピュータ、キオスク、パーソナル・デジタル・アシスタント (PDA) および自動窓口機 (ATM) 等の一般的なデバイスのユーザIDおよびパスワードに取って代わるものである。生物測定学的情報や現金の引き出しまたはクレジット・カードによる購買等のサービスに

対する要求は、ネットワークに割り当てられた普遍的な管理されたアドレス (UAA) と同様に、固有のデバイスIDに沿って製造業者のデバイスに割り当てられた復号鍵によって暗号化され、デバイスIDおよびメッセージ・ヘッダによって上流の信用サーバに転送される。サーバでは、生物測定データおよびサービス要求がデバイスの公開鍵によって解読される。このデバイスの公開鍵は、メッセージからのデバイスIDを用いて得られる。続いて、網膜スキャン、指紋等の転送されるタイプの事前に保存された生物学的データのデータベースに対して確認される。ひとたびユーザが認証されサービス要求がユーザの特権に対して確認されると、サーバは実行依頼された要求を安全に処理する。

【0006】

【発明の実施の形態】図1は、本発明にもとづく強化されたセキュリティ・システムを構築するために、遠隔地および局所の両方で使用することが可能なコンピュータ・システムの一実施形態例を示す。このシステムは、CPU10、読み出し専用メモリ (ROM) 11、ランダム・アクセス・メモリ (RAM) 12、I/Oアダプタ13、ユーザ・インタフェース・アダプタ18、通信アダプタ14、およびディスプレイ・アダプタ19を有し、これらすべては共通のアドレス／データおよび制御バスまたはバス16を介して相互に接続している。上記構成要素の各々は当業者に既知の従来の技術を用いて共通バスにアクセスし、バスマスタであるCPU10によってシステム内の各構成要素に対して特定のアドレス範囲を提供するような方法が含まれる。図1にさらに示すように、DASD15等のそれらの外部デバイスは、それぞれのアダプタ、例えばI/Oアダプタ13を介して共通バス16に接続する。他の外部デバイス、例えばディスプレイ21は、同様にディスプレイ・アダプタ19等のそれぞれのアダプタを使用してバス16とディスプレイ21または他のデバイスとの間にデータ・フローを与える。様々なユーザ・インタフェース手段がユーザ・インタフェース・アダプタ18との相互接続または利用のために提供され、図ではジョイスティック23、マウス25、キーボード17、およびスピーカおよび (または) マイクロフォン27等のそれぞれのユーザ入力デバイスに接続されている。システムは、1つ以上のアプリケーション31の実行に適応した従来のオペレーティング・システム29をさらに有する。これらのユニットの各々はそれ自体では当業者によく知られたものであることから、ここでの説明は省略する。

【0007】本発明は、本質的に任意のコンピュータ・システムおよび対応するマイクロプロセッサの実現を認める。例えば、RS/6000 (登録商標)、RISCベース・ワークステーション、AIX (登録商標) およびOS/2 (登録商標) オペレーティング・システムを各々実行するIBM Corporationのパーソナル・コンピュ

ータ、あるいは他のベンダーによる類似のハードウェアで、例えばRS/6000ワークステーションの場合は604PowerPC（登録商標）RISCチップである（RS/6000、IBM、AIX、OS/2およびPowerPCはIBM Corporationの登録商標である）。

【0008】図1のCPU10と一緒に実装されているものは、一般にシステム・アドレス、データ、および図1のシステムの動作を補正するために必要な制御処理機能を実行する1つ以上のマイクロプロセッサである。本発明は様々なマイクロプロセッサ設計に対する適用を認めるが、ここに開示する実施形態例では、マイクロプロセッサはIBM Corporationによって製造されたPowerPC604マイクロプロセッサの形態をとる。このマイクロプロセッサは、縮小命令セット・コンピュータ（RISC）マイクロプロセッサとして知られているマイクロプロセッサの一種である。そのようなマイクロプロセッサのアーキテクチャおよび動作についての詳細は、PowerPC604RISCマイクロプロセッサの取扱説明書（PowerPC 604 RISC Microprocessor User's Manual, Document #MPC604UM/AD, November, 1994, copyright IBM Corporation）（この文献を本明細書の記載の一部として援用する）から得ることができよう。

【0009】本発明によれば、ユーザは、マウスおよび音声起動ナビゲーション等の様々なポインティング・デバイス25によって操作可能であるディスプレイ21上のカーソルおよびポップ・アップまたはポップ・ダウン・メニュー等の様々なオブジェクトを見るであろう。動作環境やRAM12および（または）DASD15に常駐するアプリケーション・コードと関連してポインティング・デバイス25およびマイクロフォン27のためのデバイス・ドライバによってユーザ・インタフェース・アダプタ18に対応付けられたプログラム・コードは、マイクロフォン27に向かって話された相関的な音声コマンドに反応して、あるいは該音声コマンドと連携してディスプレイ・スクリーン21上のカーソルの動きを促進かつ可能とさせる。

【0010】図1のコンピュータ・システムに描かれた機能的構成要素を上記したように変更したり、以下に詳細に説明するローカル・デバイスおよびリモート・コンピュータ・システムの必要性および適用に適合させてもよい。例えば、ローカル・デバイスが既に述べたPDAの形態を取る場合、ジョイスティックまたはスタンドアローン型のマウスまたは他のポインティング・デバイスは不要であるか、あるいはPDAそれ自体のなかに組み込まれる。同様に、PDAの内蔵部品としてスタンドアローン型のディスプレイは不適當であり、またLCDまたは他の小さなディスプレイはより妥當であることが認められよう。逆に、キオスクまたはATM用途では、例えばそのようなスタンドアローン型のディスプレイがよ

り妥當であろう。しかし、基本的な概念は、図1の機能的構成要素を異なる形態で、あるいは必要に応じてそのような構成要素を多数必要とするかもしれない遠隔地および局所の両方でかなり多様な異なるコンピューティング・デバイスを本発明では認められるということである。したがって、本発明はいかなる特定のコンピュータ・システムに限定されるものではない。

【0011】ここで図2を再び参照しながら説明する。安全なトランザクションがもたらされるように図3のシステムによりエンド・ユーザによる使用のために製造業者がリモート・デバイスを準備してもよいから以下説明する。そのような安全性を確保するために、そのような図はさらに図3のシステムで用いられるIDおよび鍵の生成をさらに詳細に説明する。

【0012】第一に、当業者によく知られているいくつかの方法のいずれかによって、複数の公開／復号鍵対40を生成するためのプロセスが用いられよう。同様に、プロセス46は複数のデバイスIDを生成するために用いられよう。複数のデバイスIDは、図3のシステムと相互作用するリモート・ユーザによって用いられる異なった固有の物理的デバイスに各々が対応している。固有のデバイスIDは、一般にネットワーク・サーバクライアントで用いられているネットワーク・インフォメーション・カード（NIC）に対応付けられた普遍的な管理アドレス（UAA）として知られているものと類似しているだろう。それによって、各個の物理的デバイス（例えば、NIC、PDA、ATM、キオスク等）はそれ自体に対応付けられたそのようなデバイスIDを持つ。公開／復号鍵対生成プロセスからのフローは公開鍵矢印42で示される公開鍵と復号鍵矢印50で示される復号鍵となる。同様に、デバイスID生成プロセス46からのフローは矢印48および52で示されるデバイスIDとなる。プロセス40および46からのフローしたID／公開鍵としての参照符号44で示される公開鍵—デバイスID対は、矢印45で模式的に示されるように、以下に記載するように暗号化鍵データベース72（図3）に送られる。データベース72は、各々が複数の個別のデバイスの異なる1つに対して一意的である複数のそのようなID／公開鍵対44を格納する。

【0013】同様に、プロセス40および46は、復号鍵矢印50で示される複数の復号鍵とデバイスID矢印52で示されるデバイスIDとを生成する。そのような固有の復号鍵／ID対は復号鍵／ID対54として図示されている。復号鍵／ID対54は矢印56として示されるように送られ、また特に好ましくは暗号化プロセッサ・アセンブリ58の一部分を含む読み取り専用メモリ（ROM）60上に付される。各々のそのような暗号化プロセッサ・アセンブリ（EPA）58によって、特定のEPA58にのみ対応付けられた異なる固有のそのような復号鍵／ID対54を不揮発的に保持することを容

易に理解することができよう。さらに、各EPA58は適当な生物測定学的入力センサ・デバイス62と対応付けられる。このセンサ・デバイス62は指紋スキャニング・パッド、網膜または顔スキャニング・カメラ等の形をとってもよく、例えば本発明によって認証される使用を行うEPA58の特定のユーザに一意的に対応付けられた生物測定データを生じさせることが可能な任意のデバイスである。したがって、本発明は生物測定学的入力センサ・デバイスのいずれかの特定の形状に限定しようとするものではなく、むしろ特定のユーザに一意的に対応付けられ生物測定データの生成を行うことが可能な一切のデバイスによる用途を認めるものである。EPA58および生物測定学的入力センサ・デバイス62は製造元によって一緒に結合させてもよく、あるいはエンド・ユーザ・デバイス、例えばATM、キオスク、PDA等を製造する際に必要に応じて接続してもよいことは理解されよう。ちなみに、「公開」および「復号」鍵は対となった鍵の固有の異なる部分に対してのみ使われる用語であることにさらに注目しておくべきであろう。EPA58のデバイス・オペレータは「公開」鍵のみにアクセスすることが理解されよう。

【0014】ID、公開／復号鍵の生成についての説明、そのような復号鍵とIDSとを用いるデバイスがリモート・ユーザによって使用されることを説明してきた。ここで、EPAと生物測定学的入力センサ・デバイスからの入力およびそれらのID／公開鍵対44を用いる図3のシステムについてより詳細に説明する。

【0015】はじめに、図3の上側には前述した暗号化鍵データベース72が図示されている。このデータベース72は図2で生成された複数のID／公開鍵対44のためのリポジトリである。また、図3の下側部分には、既におなじみのPDA58が図示されている。このPDA58はROM60を有するもので、図2のプロセスにもとづいて生成され、かつ特定のEPA58に一意的に対応付けられた復号鍵／ID対の1つが格納されている。

【0016】さらに図3では、生物測定学的鍵データベース74が表示されている。このデータベース74は、複数の生物測定データ・ユーザ・データ・フィールド対からなる。そのような対の各々では、生物測定データは特定のエンド・ユーザに一意的に対応付けられており、さらに許可、アカウント番号等の複数のデータ・フィールドもまた特定のエンド・ユーザに一意的に対応付けられており、エンド・ユーザの生物測定データはすべてデータベース74に格納される。

【0017】図3のシステムは、さらに信用サーバ70を含む。このサーバ70の一部分は、ユーザのEPA58とのユーザ・インタラクションによって送出されたエンド・ユーザ要求に応える機能を果たす。信用サーバ70とEPA58との間に配置された適当なネットワーク

66によって、EPA58と信用サーバ70とが互いに通信しあう。このネットワークはイントラネット、インターネット、ダイヤル・アップ・ネットワーク、あるいはリモートEPA58とサーバ70とが相互接続するのに適した適当な他のネットワークのいずれかの形をとるものであってもよい。

【0018】信用サーバ70によって実行される本発明に関係した1つの重要な機能は、データベース72に格納された暗号化鍵を用いてEPA58によって生成された要求64を解釈し、データベース74に格納された生物測定データを介してユーザ許可および他のデータを認可する機能を提供することである。以下に詳細に説明するこのような要求64は、ROM60に格納されたデバイスIDデータ54および他のトランザクション・データのいずれかと同様にセンサ・デバイス62を介したユーザ入力の生物測定データを含む。このID、生物測定データおよびトランザクション・データはサーバ70へのリンク68を介してネットワーク66に送られる。2方向矢印76および78でそれぞれ示されるデータベース74とデータベース72との相互作用は、より詳細に説明されるであろう方法によってライン68を通して入ってくる暗号化されたユーザ要求の解釈を生ずる。

【0019】したがって、以上のことをまとめると、EPA58と対話するユーザは本質的に、特定のATM、キオスク、PDA等にある生物測定学的入力センサ・デバイス62を用い、EPA58によって表されるユーザの生物学的入力データを提供する。ユーザは、このように存在する生物測定データに基づいてさらに使用する確認を要求する。そのような生物測定データは、従来技術にもとづくものであろうとなかろうと損なわれやすい（例えば、悪事を行う者が正当なユーザの指紋を盗むこと等）ので、本発明の重要な特徴は特定のEPA58でこの不適当な生物測定データを使用する能力に欠けている悪事を行う者によってそのようなデータが使用されることはほとんどないので、このデータはROM60に格納された復号鍵54によってさらに暗号化され、特定のユーザに一意的に対応付けられるであることに注目することが重要である。

【0020】データベース72および74に格納されている情報を用いるサーバ70によってひとたび解釈が実行されると、確認が実行されたエンド・ユーザへの通知はサーバ70からネットワーク66へ向けてライン69上を送られ、最終的にネットワーク66からEPA58へのライン71で示されるようにEPA58を経由してエンド・ユーザに送られてもよい。その後、安全なリンクがそれによって確立され、エンド・ユーザはサーバ70と対話するように詳細を追加してもよく、それによってデータベース74のユーザ・データ・フィールドへのデータの追加を行ったり、あるいは必要に応じて特定のユーザに対応付けられたそのようなデータの検索を許可

10

20

30

40

50

したりすることも可能である。

【0021】確認機能決定ブロック80はさらに図3に示されており、有効な要求が存在するかどうかを決定するために、データベース72内の対応するID/公開鍵情報およびデータベース74内の生物測定データとライン64上に入ってくる復号鍵/ID情報を相関させることに使用される可能性がある一連の論理プロセスを機能的に表現する。したがって、本発明は確認機能決定アルゴリズム80のいかなる特定の形に限定されるものではなく、本質的にそれらの入力を適当なものとして用いるいかなる決定も許容する。入力ライン82によって確認機能決定ブロック80へ送られるものとして示されて、それからもたらされる最終的な決定は確認機能決定ブロック80からライン86を経由してサーバ70に戻る。

【0022】ここで図4に戻る。この図4に描かれているのは、EPA58を生成するのに用いられる一連のイベントを説明し、図2に関連して既に説明したような方法で生成される様々な鍵およびIDを生じさせるフローチャートである。最初に、図2の鍵生成プロセッサ40に対応して参照ブロック88で示される各々の潜在的なユーザに対して、鍵の対 K_1 、 K_2 が生成されることが再現されるだろう。同様に、複数の特有のデバイスIDが生成され、各々が異なる物理的EPA58に対応し、そのようなデバイスIDの生成はブロック90として示され、さらに図2のブロック46に対応する。その結果、複数のID、 K_1 からなる対と、複数の K_2 対を生成するために、生成されたこれらの鍵の対と特有のデバイスIDは矢印92および94とブロック96とに示すように結合する。IDの K_2 対はライン114に示すように送られ、引き続いて起こるEPA58の購入者への転送のために暗号化鍵データベース72に格納される。ID、 K_2 対の格納はブロック116に示される。デバイス・オペレータがEPA58を獲得あるいは購入した場合、一意のID、 K_2 対が送られ、ブロック120のライン118で示すように、または最終結合デバイス・オペレータに送られ、そこからライン122で示すように、ID K_2 対はブロック124で示される様々なIDで鍵がかけられたデータベース72に置かれる。このようにして、EPAに対応する特定のEPA58をエンド・ユーザが用いる場合、データベース72に常駐する一意的なIDと公開鍵とが存在する。

【0023】図4を参照しながらさらに説明する。ID K_2 対と同じようにして、ID K_1 対は矢印98に模式的に示したように、一意的に対応付けられたEPA58に送られ、それによってID K_1 は特定のEPA58上のROM60に書き込まれる。このことは図4のブロック100で示されている。このID K_1 対がROM60に「書き込まれる(burned)」と表現されるのに対して、重要な点は特定のEPA58に一意的に対応付けられた

ID K_1 データはEPA58に不揮発的に格納されることである。したがって、本発明は、このような目標に達成するために数多くの様々な方法のいずれかを許容するもので、その中のほんの1例としてフラッシュ・バイオス、E²PROM、ソケットにはめられたROMの物理的交換等によって実際に「書き込む(burn)」。

【0024】図4を参照しながらさらに説明する。ひとたびこのID K_1 データが特定のEPA58に関連して不揮発的に格納されると、プロセスはフロー120によって示されるように続行し、この特定のEPA58が選択される生物測定学的入力デバイス62と結合され、そのような結合は図4においてブロック104として表される。この結合は、例えば、生物測定学的入力デバイス62と対話する特定のユーザに関する生物測定データとROMのデータ(例えば、復号鍵/ID対54)とを含む電気的に生じた要求を提供することが可能なように、電気的およびソフトウェア的に、ROM60と生物測定学的入力センサ・デバイス62とが統合されることのみを意味する。

【0025】ひとたびこのEPAと生物測定学的入力デバイスとがそのように電気的に「結合(coupled)」されてアセンブリを形成すると、該結合アセンブリは前述したATM、キオスク、PDA等であろうとなかろうと適当な末端デバイス108に取り付けられ、かつ該デバイス108とアセンブルされる。

【0026】最後に、フロー110によって示されるように、キオスクをショッピング・モールに据え付けたり、ATM機械をドライブ・スルー・バンクに据え付けたり、PDAをエンド・ユーザに販売したりするなど、このような所望のデバイスに設けられた結合アセンブリの配置を行う。

【0027】ここで図5を参照しながら説明する。この図は、図3に示されたシステムのトランザクション許可の流れを説明するためのフローチャートである。ここでは、上記したような様々な鍵、ID、データベースおよびEPAが使用され、エンド・ユーザはネットワーク66を介してサーバ70にトランザクションを生成し、安全な許可を受け取ることが可能である。はじめに、使用中、デバイス・オペレータによって生物測定データを同様の生物測定学的入力センサを介して登録するために、ユーザはEPAのオペレータと対話する。ひとたび登録されると、使用中、ユーザは適当な生物測定データを入力(126)、EPA(網膜スキャナ、指紋スキャナ等)を付属する特定のトランスデューサによってもらい制御され、フローが継続する。フローは矢印128に沿ってブロック130へと続く。ブロック130で示されるこの地点で、オペレータは、既に述べた関連記録データ(例えば、アカウント番号、許可等の既に指摘したデータ・フィールド)に沿って第2または生物測定データベース74の鍵としてブロック126にもとづいて、そ

のようにして得られた生物測定データを利用する。フローは、さらに矢印132に沿ってブロック134に続く。このブロック134では、ユーザはトランザクション許可を要求するように生物測定データ入力デバイスに結合したEPAを用いる。つぎに、フローは矢印136に沿ってブロック138に続く。このブロック138は入力生物測定データとトランザクション・データとの組み合わせを第1の鍵K₁を用いて暗号化されたメッセージのなかに表す。

【0028】図5を参照しながらさらに説明する。フローは矢印140に沿ってブロック142に続く。このブロック142は、EPA58のシステムがその後、ROM60に格納されたIDをクリア・テキストで要求メッセージに付加するという意味を表す。フローは矢印144に沿ってブロック146に続く。このブロック146は、その後の解読のために、そのようにコンパイルされたメッセージが要求64としてネットワーク66介し、かつコネクション68によってサーバ70へ送られることを示す。

【0029】フローはつぎに矢印148に沿ってブロック150に続く。このブロック150は機能的に信用サーバ70を表すもので、EPAIDをはがし、それをデータベース72に対応付けられたユーザの鍵K₂の検索に用いる。ひとたびこのことが完了すると、フローは矢印152に沿って続き、ブロック154で、この鍵K₂は既に記載されたブロック138に従ってK₁メッセージによって事前に暗号化されているメッセージを解読するのに使われる。フローは矢印156に沿ってブロック158に続く。このブロック158は、確認機能80にその後要求されたメッセージが送られることを示す。フローは矢印160に沿ってブロック162に続く。このブロック162は、生物測定データベース74からのユーザ・データを検索するために鍵としてメッセージの生物測定学的部分を用いる確認機能のステップを示す。フローは矢印164に沿ってブロック166に続く。このブロック166では、確認機能80は矢印82に沿ってサーバ70から受け取ったこのデータに基づいて認証決定を下す。確認機能はK₂鍵による場合と同様に任意に応答を暗号化して、矢印86に示されるように元のデバイスに送り戻すことが可能であるという点が注目されよう。つぎにフローは矢印168に沿ってブロック170に続く。このブロックは、サーバ70の機能を表すもので、その後、確認されている要求の結果としての応答をネットワーク66を通してEPA58を用いるエンド・ユーザに送る。そこで応答を、既知のK₁鍵で任意に解読(ステップ166で暗号化されている場合)することができると、デバイス58はこの認証決定データに作用することが可能であろう。

【0030】本発明の真の精神から逸脱することなく本発明の好ましい実施形態例に種々の修飾または変化を加

えることが可能であることは上記の説明から理解されよう。この発明の詳細な説明の記載が説明することのみを目的として記述されたもので、限定的な意味で解釈されるべきではないことが意図されている。この発明の範囲は特許請求の範囲によってのみ限定される。

【0031】まとめとして、本発明の構成に関して以下の事項を開示する。

(1) コンピュータ・システム・ネットワークでユーザの要求を認証するための方法であって、復号鍵および公開鍵を生成するステップと、前記ユーザに対応する生物測定データを生成するステップと、遠隔地で前記生物測定データと前記公開鍵とを記憶するステップと、前記復号鍵によって暗号化された前記生物測定データを含む前記ユーザ要求を局所で生成するステップと、前記遠隔地に前記ユーザ要求を伝送するステップと、前記遠隔地で前記公開鍵を用いて前記ユーザ要求を前記生物測定データに解読するステップと、前記記憶された生物測定データを検索するステップと、前記ユーザ要求を認証するために前記生物学的測定データを確認するステップと、を有することを特徴とする方法。

(2) 前記生物学的測定データを確認するステップは、前記解読されたユーザ要求に送られた前記生物測定データと前記記憶された生物測定データとを比較することを含むことを特徴とする上記(1)に記載の方法。

(3) 前記ユーザ要求の伝送は、前記局所と前記遠隔地とを相互接続するネットワーク上であることを特徴とする上記(2)に記載の方法。

(4) 前記復号鍵に対応付けられたID番号を持つ前記遠隔地の前記復号鍵を記憶するステップを、さらに有することを特徴とする上記(3)に記載の方法。

(5) 前記ID番号は前記公開鍵に対して一意的に対応付けられており、前記方法はさらに、前記ID番号および前記公開鍵を前記遠隔地の第1のデータベースに組として記憶するステップを有することを特徴とする上記(4)に記載の方法。

(6) 前記生物測定データは第2のデータベースに記憶されていることを特徴とする上記(5)に記載の方法。

(7) 前記ユーザおよび前記生物測定データに対応付けられたデータ・フィールドを生成するステップと、前記生物測定データと前記データ・フィールドとを組として前記第2のデータベースに記憶するステップと、をさらに有することを特徴とする上記(6)に記載の方法。

(8) 前記復号鍵を記憶するステップは、前記局所で行われることを特徴とする上記(7)に記載の方法。

(9) 前記生物測定データを生成するステップは、前記局所で行われることを特徴とする上記(8)に記載の方法。

(10) 前記確認に応じて前記要求を処理するステップをさらに有することを特徴とする上記(9)に記載の方法。

(11) コンピュータ・システム・ネットワークでユーザの要求を認証する装置であって、復号鍵および公開鍵を生成する手段と、前記ユーザに対応する生物測定データを生成する手段と、遠隔地で前記生物測定データと前記公開鍵とを記憶する手段と、前記復号鍵によって暗号化された前記生物測定データを含む前記ユーザ要求を局所で生成する手段と、前記遠隔地に前記ユーザ要求を伝送する手段と、前記遠隔地で前記公開鍵を用いて前記ユーザ要求を前記生物測定データに解読する手段と、前記記憶された生物測定データを検索する手段と、前記ユーザ要求を認証するために前記生物学的測定データを確認する手段と、を有することを特徴とする装置。

(12) 前記生物学的測定データを確認する手段は、前記解読されたユーザ要求に送られた前記生物測定データと前記記憶された生物測定データとを比較する手段を含むことを特徴とする上記(11)に記載の装置。

(13) 前記ユーザ要求を伝送する手段は、前記局所と前記遠隔地とを相互接続するネットワーク上であることを特徴とする上記(12)に記載の装置。

(14) 前記復号鍵に対応付けられたID番号を持つ前記遠隔地の前記復号鍵を記憶する手段を、さらに有することを特徴とする上記(13)に記載の装置。

(15) 前記ID番号は前記公開鍵に対して一意に対応付けされており、前記装置はさらに、前記ID番号および前記公開鍵を前記遠隔地の第1のデータベースに組として記憶する手段を有することを特徴とする上記(14)に記載の装置。

(16) 前記生物測定データを前記遠隔地で第2のデータベースに記憶する手段をさらに有することを特徴とする上記(15)に記載の装置。

(17) 前記ユーザおよび前記生物測定データに対応付けられたデータ・フィールドを生成する手段と、前記生物測定データと前記データ・フィールドとを組として前記第2のデータベースに記憶する手段と、をさらに有することを特徴とする上記(16)に記載の方法。

(18) 前記復号鍵の記憶は、前記局所で行われることを特徴とする上記(17)に記載の装置。

(19) 前記生物測定データの生成は、前記局所で行われることを特徴とする上記(18)に記載の装置。

(20) 前記確認に応じて前記要求を処理する手段をさらに有することを特徴とする上記(19)に記載の装置。

【図面の簡単な説明】

【図1】PDA等の一般的なリモート・デバイスからなる手段によって対話する本発明の具体化した部分であるリモート・コンピュータ・システムの高度に機能的なブロック図である。

【図2】リモート・ユーザ・デバイスが本発明にもとづいて構成される手順を説明するための機能的なブロック

図である。

【図3】図2に示すデバイスによって本発明にもとづいて対話するリモート・システムの構成要素を表す機能的なブロック図である。

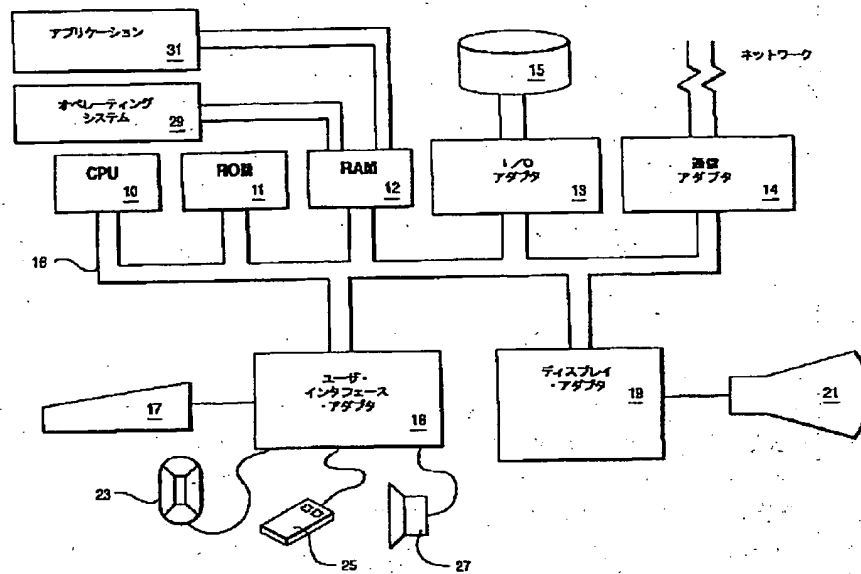
【図4】図2のリモート・ユーザ・デバイスが生成されるステップとセキュリティ情報を有する図3のシステムとを説明するためのフローチャートである。

【図5】所望の安全なトランザクション許可をもたらすように図2のデバイスが図3のシステムと対話する場合のイベントの順序を説明するためのフローチャートである。

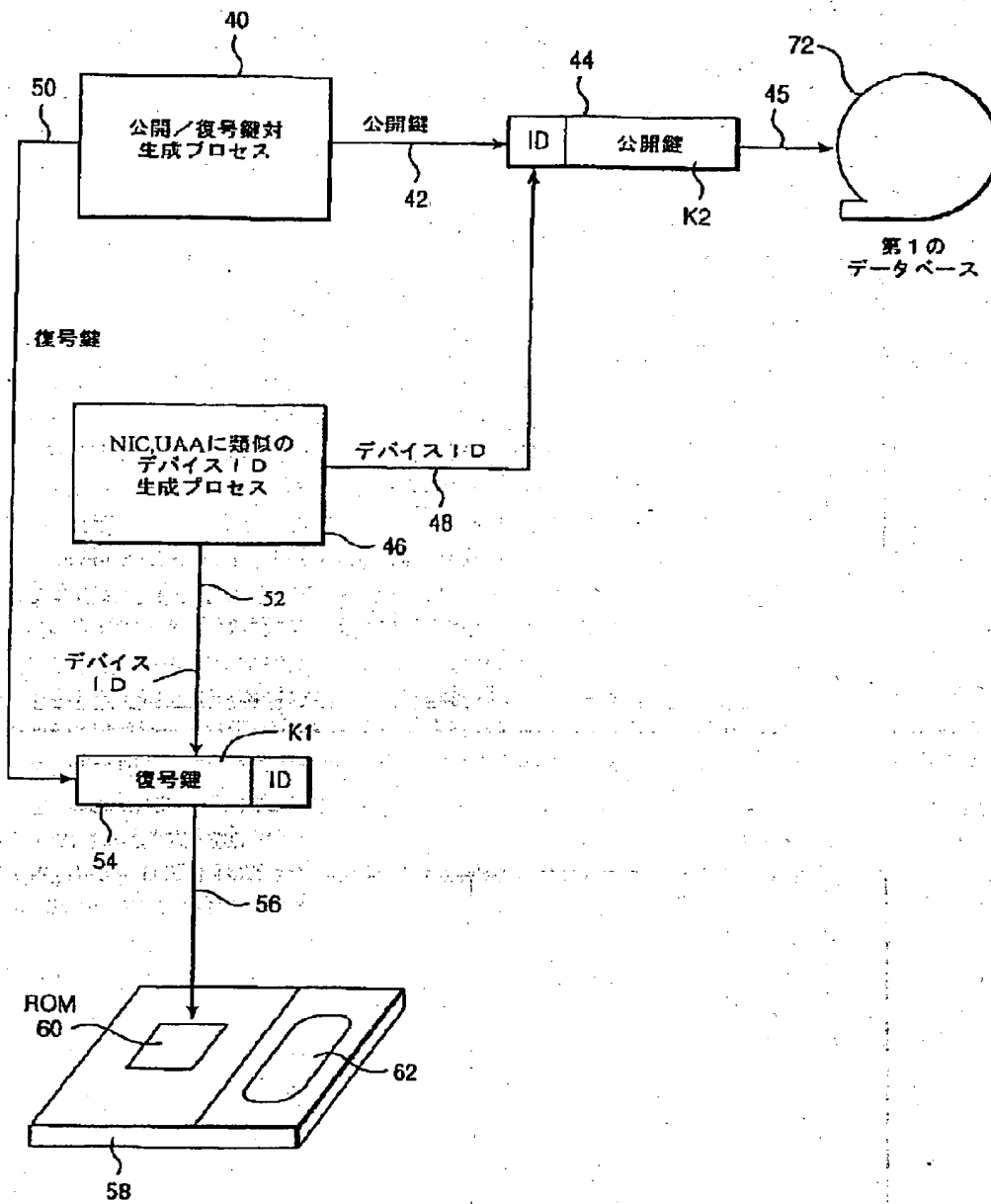
【符号の説明】

10	CPU
11	ROM
12	RAM
13	I/Oアダプタ
14	通信アダプタ
15	DASD
16	バス
17	キーボード
18	ユーザ・インタフェース・アダプタ
21	ディスプレイ(ディスプレイ・スクリーン)
23	ジョイ・スティック
25	ポインティング・デバイス(マウス)
27	スピーカおよび(または)マイクロフォン
29	オペレーション・システム
40	公開/復号鍵対の生成プロセス
42	矢印
44	公開鍵-復号鍵対
45	矢印
46	デバイスID生成プロセス
48	矢印
50	矢印
54	復号鍵-ID対
56	矢印
58	暗号化プロセッサ・アセンブリ(EPA)
60	ROM
62	生物測定的入力センサ・デバイス
64	要求
66	ネットワーク
68	リンク
70	信用サーバ
72	データベース
74	データベース
76	矢印
78	矢印
80	確認機能決定ブロック
86	矢印

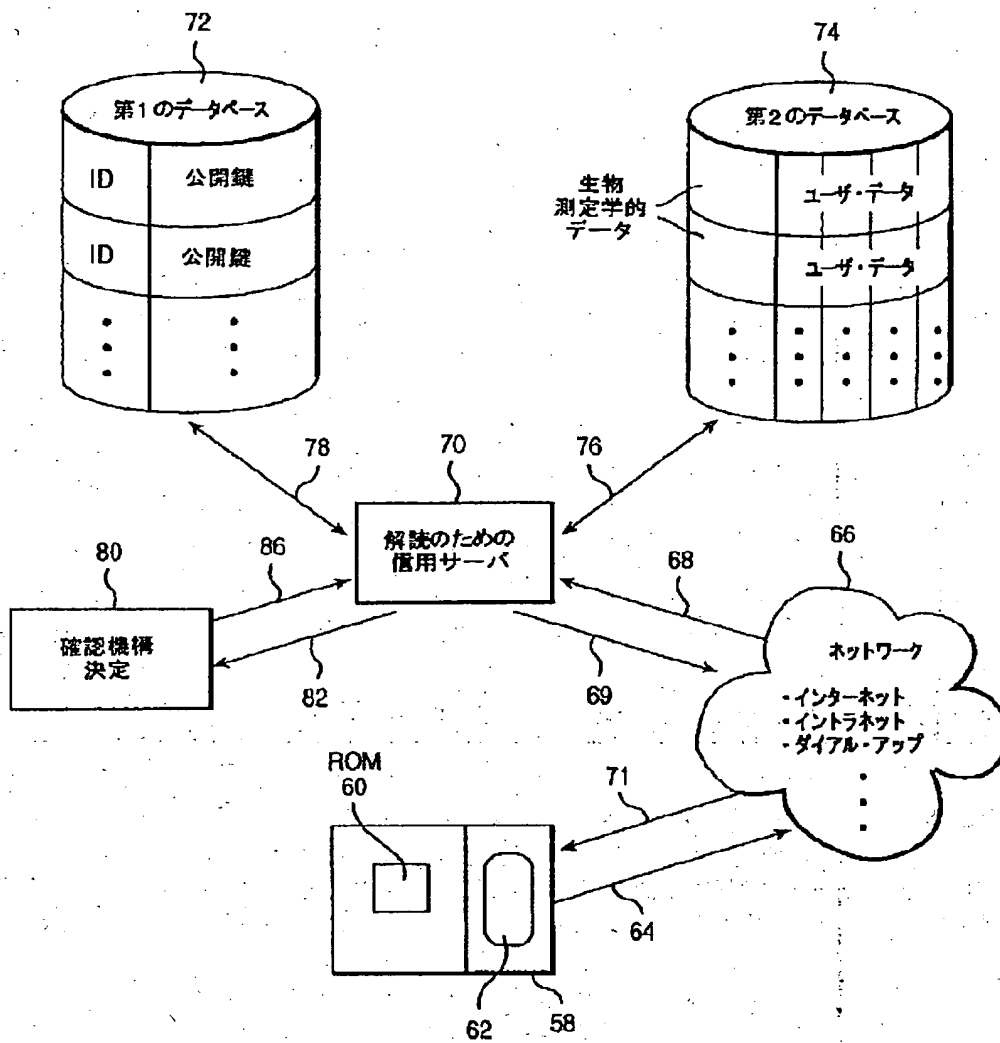
【図1】



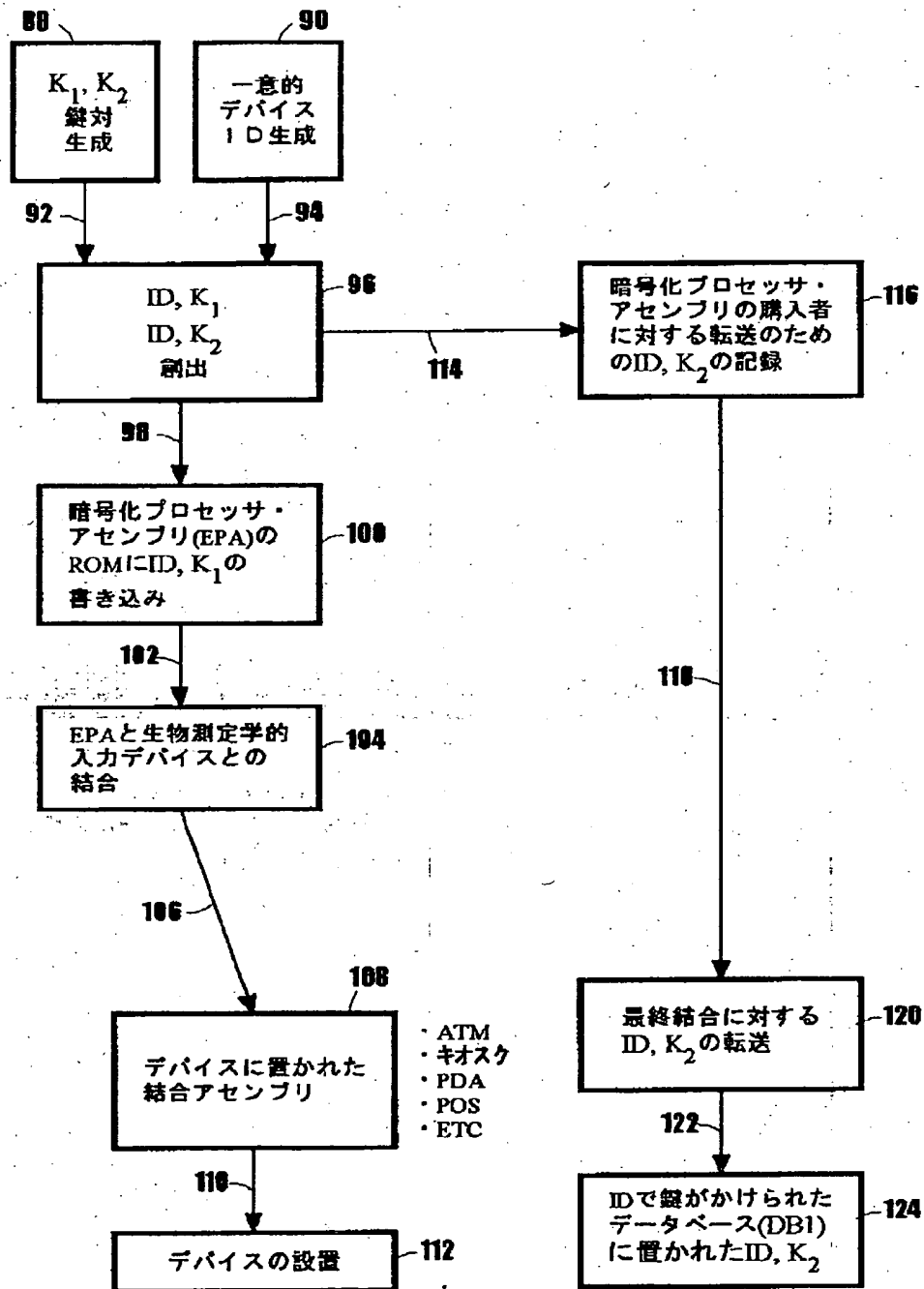
【図2】



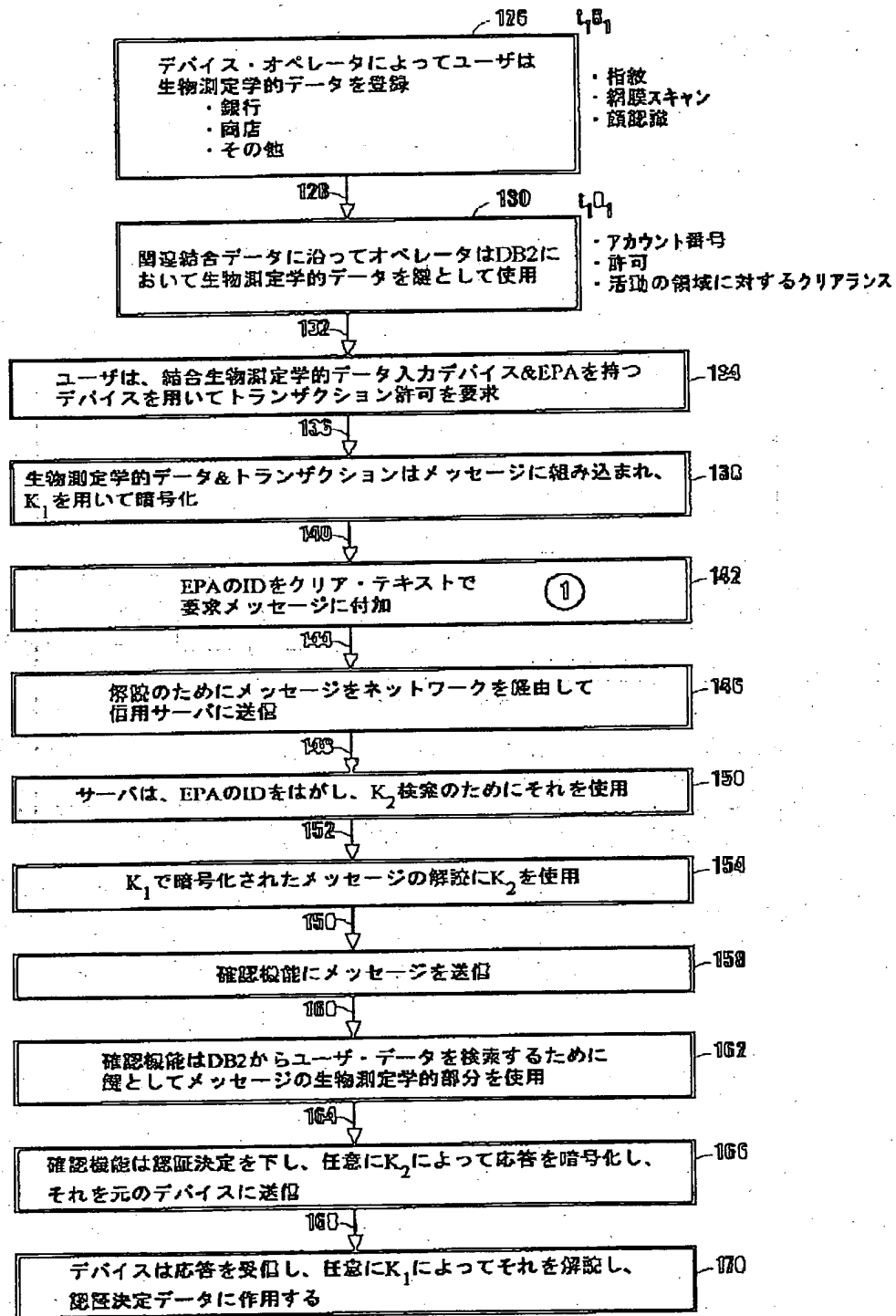
【図3】



【図4】



【図5】



(14)

特開2000-181871

フロントページの続き

(51)Int.Cl.⁷

識別記号

F I

テーマコード(参考)

H 0 4 L 9/00

6 7 5 B

BEST AVAILABLE COPY